

REMARKS/ARGUMENTS

Favorable reconsideration of this application in light of the following discussion is respectfully requested.

Claims 1, 3-5, 7, 9, 11 and 13-18 are pending in the present application. No claim amendments are presented, thus no new matter is added.

In the Office Action, Claims 1, 3-5, 7, 9 and 11-18 are rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Pat. 6,248,946 to Dwek in view of U.S. Pub. 2001/0051996 to Cooper et al. (herein, Cooper).

Applicants respectfully traverse the above noted rejection under 35 U.S.C. § 103, as independent Claims 1, 9 and 13 recite novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1, for example, recites, in part, a user authentication method for an authentication server which executes user authentication between a mobile information terminal and a content providing server interconnected by an open network, comprising:

... transmitting, from said authentication server to said mobile information terminal, a certificate including a public key of the authentication server, an expiration date of the certificate and a digital signature;

verifying an identity of the authentication server at the mobile information terminal based on the received certificate;

generating, *at a Web browser of the mobile information terminal, a secret key based on a result of the verification;*

encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server;

transmitting the encrypted secret key from the mobile information terminal to the authentication server;

receiving, at the authentication server from said mobile information terminal, the unique identification information as encrypted by said secret key at the Web browser installed on said mobile information terminal, and a request for registering one of said official site access information for accessing said content providing server with a personal menu via a network ...

Independent Claims 9 and 13, while directed to alternative embodiments, recite similar features.

At pp. 4-5, the Office Action concedes that Dwek fails to disclose the above emphasized features recited in independent Claim 1. In an attempt to remedy these deficiencies, the Office Action relies on various portions of Cooper and asserts that it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the cited references to arrive at Applicant's claims. Applicant respectfully traverses this rejection, as Cooper fails to disclose the claimed features for which it is asserted as a secondary reference under 35 U.S.C. § 103.

At paragraph [0135], Cooper describes a process of issuing two encryption keys to a user over a network. This Public Key Infrastructure (PKI) information consists of a pair of keys, a public key and a private key. The public key can be published to friends and partners around the world, and the private key is always kept on only one computer, mobile phone, hand-held device, television set, or other user device 115. Moreover, paragraphs [0145-0148] of Cooper do appear to describe that a digital certificate may be issued from a server to a customer device, and that the certificate is used to verify the customer device as a trusted device.

Cooper, therefore, describes that the private key (e.g. secret key) is issued to a user over a network, and fails to teach or suggest “**generating**, at a Web browser of the mobile information terminal, **a secret key based on a result of the verification**”, much less “**encrypting**, at the Web browser of the mobile information terminal, **the generated secret key using the public key of the server**”, as recited in independent Claim 1.

In rejecting the claimed features directed to generating the secret key at the mobile terminal, the Office Action relies on paragraphs [0197-0198], [0227] and [0277] of Cooper. Paragraphs [0197-0198] of Cooper describe a process of adding a transactional ID or

consumer identification data within a watermark included in content transmitted from a customer site 270 to a user device 115. Thus, this cited portion of Cooper fails to discuss generating any type of key at the user device 115. Paragraph [0227] of Cooper explicitly supports the position that the user's private key is issued by the Certificate Authority (CA) as described in paragraph [0225] and is not “generat[ed], at a Web browser of the mobile information terminal, ... based on a result of the verification”, as claimed. Finally, paragraph [0277] of Cooper describes a transactional database 214 that is used to store a customer certificate and each key used in watermarking digital content. This cited portion of Cooper further describes that stored customer certificate data contains all fields used to create an original customer certificate as well as the resulting certificate and public key. Therefore, this cited portion of Cooper merely describes a process of storing public key data and key data used for watermarking digital content transmitted from a customer site 270 to a user device 115 in a database, and fails to teach or suggest a process of generating a secret key at the user device 115, whatsoever.

Therefore, Cooper fails to teach or suggest “**generating**, at a Web browser of the mobile information terminal, **a secret key based on a result of the verification**”, as recited in independent Claim 1.

Regarding the claimed feature directed to encrypting the generated secret key using the public key and transmitting the encrypted secret key from the mobile information terminal to the authentication server, the Office Action relies on paragraphs [0218], [0227], [0225] and [0277] of Cooper.

Paragraph [0218] of Cooper merely describes a process of using an appropriate key to unlock received DRM protected data, and is in no way related to encrypting and transmitting anything, much less encrypting a generated secret key using a public key, as claimed. As discussed above, paragraphs [0225] and [0227] of Cooper describe a process of signing a

transactional ID (received as part of a process of downloading data) using a user's private key issued by a Certificate Authority (CA). Therefore, at best, this cited portion of Cooper describes using a received, or issued (i.e. not generated), private key to retrieve content data from the customer site 270, but is in no way related to "***encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server***" [and] transmitting the encrypted secret key from the mobile information terminal to the authentication server", as recited in independent Claim 1. As discussed above, paragraph [0277] of Cooper merely describes a database used to store various certificate and key information, and does not disclose a process of encrypting and transmitting, as differentiated above.

Therefore, Dwek and Cooper, even if combined, fail to teach or suggest at least the features of "***generating, at a Web browser of the mobile information terminal, a secret key based on a result of the verification ... encrypting, at the Web browser of the mobile information terminal, the generated secret key using the public key of the server ...***" [and] transmitting the encrypted secret key from the mobile information terminal to the authentication server", as recited in independent Claim 1.

Accordingly, for at least the reasons discussed above, Applicant respectfully requests that the rejection of Claim 1 (and the claims that depend therefrom) under 35 U.S.C. § 103 be withdrawn. For substantially similar reasons, it is also submitted that independent Claims 9 and 13 (and the claims that depend therefrom) patentably define over Dwek and Cooper.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 1, 3-5, 7, 9, 11 and 13-18 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, L.L.P.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Andrew T. Harry
Registration No. 56,959

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)